

CLAIMS

1. A method of authentication for Media Gateway, characterized in that the method comprises:

setting up an initial key for validating initial digital signatures between a Media Gateway and a Media Gateway Controller;

generating a new shared key having a specific lifetime by performing signaling communication between said Media Gateway and said Media Gateway Controller with said initial key;

authenticating calls and responses between said Media Gateway and said Media Gateway Controller with said new shared key; and

updating said shared key between said Media Gateway and said Media Gateway Controller if the lifetime of said shared key is expired.

2. The method according to claim 1, characterized in that the step of generating a new shared key further comprises:

initiating a register signaling from said Media Gateway to said Media Gateway Controller to register, wherein said register signaling has a parameter for generating a shared key and a digital signature generated by said initial key;

generating a shared key and setting up a lifetime of said shared key after said Media Gateway Controller has validated said Media Gateway with said initial key;

initiating a modification command from said Media Gateway Controller to said Media Gateway, wherein said modification command has a parameter for generating the shared key, a digital signature generated by said initial key and a lifetime of a shared key; and

generating the shared key and setting up the lifetime of said shared key after said Media Gateway has validated said Media Gateway Controller with said initial key.

3. The method according to claim 1, characterized in that the step of authenticating further comprises:

for each call, attaching a digital signature to each call message from said Media Gateway Controller to said Media Gateway by using said shared key;

validating said digital signature in said call message in said Media Gateway by using said shared key, and if it is valid, returning a response message attached with a digital signature using said shared key to said Media Gateway Controller; and

validating said digital signature in said response message in said Media Gateway Controller by using said shared key, if it is valid, setting up a call service, otherwise denying the call.

4. The method according to claim 1, characterized in that the step of updating said shared key further comprises:

sending a notification command from said Media Gateway to said Media Gateway Controller, requesting said Media Gateway Controller to generate a new shared key, wherein said notification command has a parameter for generating a shared key and a digital signature generated by an initial key;

generating a new shared key and setting up a lifetime of said shared key after said Media Gateway Controller has validated said Media Gateway with said initial key;

initiating a modification command from said Media Gateway Controller to said Media Gateway, wherein said modify command has a parameter for generating the shared key, a digital signature generated by said initial key and the lifetime of the shared key; and

generating the shared key and setting up the lifetime of said shared key after said Media Gateway has validated said Media Gateway Controller with said initial key.

5. The method according to claim 2, 3 or 4, characterized in that the algorithm used to generate a shared key by said Media Gateway Controller and said Media Gateway is different from the algorithm used to generate a digital signature by said Media Gateway Controller and said Media Gateway.

6. The method according to claim 2, 3 or 4, characterized in that a field/packet of an expanded protocol is used to transmit said parameter for generating a shared key and said digital signature.

7. The method according to claim 1, characterized in that the lifetime of said shared key is time, or the number of times said shared key can be used for authentication.